BRENNAN
CENTER
FOR JUSTICE

STRENGTHENING THE AMERICAN PRIVACY RIGHTS ACT

Congress should modify the American Privacy Rights Act to ensure government agencies cannot purchase Americans' sensitive data from data brokers.

Privacy laws in this country are badly outdated, creating gaps that data brokers and government agencies can exploit. The lack of a comprehensive data privacy protection law in the United States and a reliance on "notice-and-consent" regimes have spawned a market for companies to trade in Americans' personal data, including detailed location information, health information, purchase history, and browsing history. Data brokers gather information from mobile apps, cookies, and other sources that, alone or combined, can reveal the most intimate details of our lives: our movements, habits, associations, health conditions, and ideologies.

Data brokers sell this information not only to advertisers, but also to stalkers, scammers, and foreign actors. They also exploit legal loopholes to **sell Americans' personal information to government agencies, allowing agencies to bypass legal privacy safeguards.** Government agencies have argued that they can even circumvent the warrant requirement imposed by the Supreme Court for location information by simply purchasing the data. The government can use this information to exercise its coercive powers, including the ability to arrest, imprison, deport, tax, fine, and even use lethal force.

The facts are alarming:

- The list of federal agencies that reportedly have bought access to Fourth Amendment-protected location data includes the FBI, the Drug Enforcement Administration, multiple components of the Department of Homeland Security (including Customs and Border Protection, Immigration and Customs Enforcement, and the Secret Service), and the Department of Defense. Even the Internal Revenue Service has reportedly purchased access to a commercial database that contains the locations of millions of Americans' cellphones.
- Data brokers collect and sell information about activities protected by the U.S. and/or state constitutions. For instance, brokers have sold location information of people visiting abortion providers and could easily do the same for people visiting gun stores.
- The Department of Defense purchased "granular location data" harvested from a popular Muslim prayer app used by 98 million people around the world, including Americans, as well as similar data generated by a Muslim dating app.
- A report commissioned by the Office of the Director of National Intelligence warned that no one in the intelligence community knows precisely what information has been purchased or how it is used.

Modifications to APRA to Close the Data Broker Loophole

The American Privacy Rights Act (APRA) rightly seeks to restrict data brokers from exploiting gaps in our privacy laws. APRA would prohibit companies from collecting or transferring personal information unless necessary to provide a service requested by an individual or to achieve certain "permissible purposes." This would reduce the amount of personal information flowing into and out of the hands of data brokers, and it would significantly rein in the *private* market in Americans' personal data.

But APRA contains exclusions and exceptions that make it far too easy for *government* agencies to purchase Americans' sensitive information. These shortcomings in the bill—and the solutions to them—are as follows:

- APRA largely excludes government service providers from its coverage, which it defines as entities that collect, process, retain, or transfer data on behalf of a government entity. This broad carveout would exempt nearly all government purchases of data from data brokers.
    - *Solution:* Government service providers must be covered under the bill. Legitimate governmental uses of Americans' data should be addressed through tailored exceptions to the bill's prohibitions, not a categorical exclusion.
- APRA contains broad law enforcement-related exceptions in its list of permissible purposes that could leave open avenues for law enforcement and intelligence agencies to acquire personal information without sufficient justification or legal process.
    - *Solution:* These exceptions should be narrowed to prohibit transfers of data to law enforcement or intelligence agencies absent clear indications of a threat to public safety, a security incident, fraud, harassment, or criminal activity, or unless the government has followed the legal process required for compelled disclosure.

A separate bipartisan bill that passed out of the House, the Fourth Amendment Is Not For Sale Act, would go a long way toward appropriately limiting governmental purchases of Americans' data. But that bill would not cover certain sensitive information like health, financial, or biometric information. A strengthened APRA can help fill those gaps.

Placing reasonable conditions on law enforcement access to data would not risk public safety or block law enforcement from accessing information for investigations. These measures would simply ensure that the data broker loophole cannot be used to evade constitutional and statutory protections for sensitive information. There is no evidence that complying with these longstanding privacy protections is harmful to public safety.

This solution has popular support. **Recent polling shows that 80% of Americans support requiring the government to obtain a warrant before purchasing location information, internet records, and other sensitive data about Americans.**

For questions about strengthening the American Privacy Rights Act, contact Liza Goitein at goiteine@brennan.law.nyu.edu or Emile Ayoub at ayoube@brennan.law.nyu.edu.